## CLAIMS

1. A system comprising:

a set of filters;

a mapping of virtual addresses to network addresses; and

a controller, coupled to the set of filters and the mapping, to,

access, upon receipt of a data packet requested to be sent from a computing device to a target device via a network, the set of filters and determine whether the data packet can be sent to the target device based on whether the computing device is allowed to communicate with the target device,

replace, based on the mapping, the target address in the data packet with a corresponding target network address; and

forward the data packet to the target device at the target network address if it is determined the data packet can be sent to the target device.

2. A system as recited in claim 1, wherein the controller is further to prevent the computing device from modifying any of the filters in the set of filters.

3. A system as recited in claim 1, wherein the computing device includes the system.

**4.** A system as recited in claim 1, wherein the controller is to make the computing device aware of the virtual addresses in the mapping but to hide the network addresses in the mapping from the computing device.

**5.** A system as recited in claim 1, wherein the controller is further to allow the set of filters to be modified by a plurality of remote devices operating at a plurality of different managerial levels.

**6.** A system as recited in 5, further comprising allowing the set of filters to be modified by a lower managerial level remote device only if the modifications are not less restrictive than modifications imposed by a higher managerial level remote device.

**7.** A method comprising:

maintaining, at a computing device, a set of filters that restrict the ability of the computing device to communicate with other computing devices;

allowing the set of filters to be modified from a remote device; and

preventing the computing device from modifying the set of filters.

**8.** A method as recited in claim 7, wherein restriction of the ability of the computing device to communicate with other computing devices comprises restricting the computing device from transmitting data packets to one or more other computing devices.

**9.** A method as recited in claim 7, wherein modification of the set of filters includes one or more of: adding a new filter to the set of filters, deleting a filter from the set of filters, and changing one or more parameters of a filter in the set of filters.

**10.** A method as recited in claim 7, wherein one or more filters in the set of filters restrict one or more of the transmission of data packets of a particular type from the computing device and reception of data packets of a particular type at the computing device.

**11.** A method as recited in claim 7, wherein one or more filters in the set of filters restrict one or more of the transmission of Internet Protocol (IP) data packets from the computing device and reception of IP data packets at the computing device based on one or more of: a source address, a destination IP address, a source port, a destination port, and a protocol.

**12.** A method as recited in claim 7, wherein one or more filters in the set of filters identifies that a data packet targeting a particular address can be transmitted from the computing device to the addressed device, and further identifies a new address that the particular address from the data packet is to be changed to prior to being communicated to the addressed device.

**13.** A method as recited in claim 7, wherein one of the filters in the set of filters is a permissive filter that indicates a data packet can be passed to its targeted destination device if the data packet parameters match corresponding parameters of the filter.

**14.** A method as recited in claim 7, wherein one of the filters in the set of filters is an exclusionary filter that indicates a data packet cannot be passed to its targeted destination device if the data packet parameters match corresponding parameters of the filter.

**15.** A method as recited in claim 7, wherein the allowing comprises allowing the set of filters to be modified by a plurality of remote devices operating at a plurality of different managerial levels.

**16.** A method as recited in 15, further comprising allowing the set of filters to be modified by a lower managerial level remote device only if the modifications are not less restrictive than modifications imposed by a higher managerial level remote device.

**17.** A method as recited in claim 7, wherein each filter includes a plurality of filter parameters, and wherein each of the plurality of filter parameters can include wildcard values.

**18.** A method as recited in claim 7, wherein the set of filters restrict the ability of the computing device to communicate with other computing devices on a per-data packet basis, wherein each filter includes a plurality of filter parameters, and wherein each filter parameter includes a filter value and a mask value indicating which portions of the filter value must match a corresponding parameter in a data packet for the data packet to satisfy the filter.

**19.** One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 7.

**20.** A network mediator comprising:

a set of filters; and

a controller, coupled to the set of filters, to,

access, upon receipt of a data packet requested to be sent from a computing device to a target device via a network, the set of filters and determine whether the data packet can be sent to the target device based on whether the computing device is allowed to communicate with the target device, and

preventing the computing device from modifying any of the filters in the set of filters.

**21.** A network mediator as recited in claim 20, wherein the controller is further to access, upon receipt of another data packet from another target device via the network, the set of filters and determine whether the data packet can be received at the computing device based on whether the computing device is allowed to receive communications from the other target device.

**22.** A network mediator as recited in claim 20, wherein the modifying of a filter includes one or more of: adding a new filter to the set of filters, deleting a filter from the set of filters, and changing one or more parameters of a filter in the set of filters.

**23.** A network mediator as recited in claim 20, wherein the network mediator is coupled to the computing device.

**24.** A network mediator as recited in claim 20, wherein the computing device includes the network mediator.

**25.** A network mediator as recited in claim 20, wherein each filter in the set of filters includes a plurality of filter parameters, and wherein each filter parameter includes a filter value and a mask value indicating which portions of the filter value must match a corresponding parameter in the data packet for the data packet to satisfy the filter.

**26.** A network mediator as recited in claim 25, wherein the controller is to allow the data packet to be forwarded to the target device if the data packet satisfies the filter.

**27.** A network mediator as recited in claim 25, wherein the controller is to prevent the data packet from being forwarded to the target device if the data packet satisfies the filter.

**28.** A method comprising:

maintaining a set of filters that restrict the ability of a computing device to communicate with other computing devices;

allowing multiple remote computing devices, each corresponding to a different managerial level, to modify the set of filters; and

preventing a lower managerial level device from modifying the set of filters in a manner that would result in a violation of a filter added by a higher managerial level device.

**29.** A method as recited in claim 28, wherein the preventing comprises:

receiving a request from the lower managerial level device to modify the set of filters;

determining whether the requested modification would result in a violation of a filter previously added to the set of filters by the higher managerial device; and

performing the requested modification if the requested modification would not result in a violation, and otherwise not performing the requested modification.

**30.** A method as recited in 29, wherein the requested modification comprises one or more of: adding a filter to the set of filters, modifying a filter in the set of filters, and deleting a filter from the set of filters.

**31.** A method as recited in claim 28, wherein the violation occurs if the modification would result in a filter being less restrictive that the filter added by the higher managerial level device.

**32.** A method as recited in claim 28, further comprising preventing the computing device from modifying the set of filters.

**33.** A method as recited in claim 28, wherein the set of filters restrict the ability of the computing device to communicate with other computing devices on a per-data packet basis, wherein each filter includes a plurality of filter parameters, and wherein each filter parameter includes a filter value and a mask value indicating which portions of the filter value must match a corresponding parameter in a data packet for the data packet to satisfy the filter.

**34.** One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 28.

**35.** One or more computer-readable media having stored thereon a computer program to implement a multiple-level filter administration scheme and including a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform acts including:

allowing a first computing device operating at a first of the multiple levels to modify a set of filters corresponding to a filtered device; and

allowing a second computing device operating at a second of the multiple levels to modify the set of filters only if the modification is at least as restrictive as the filters imposed by the first computing device.

**36.** One or more computer-readable media as recited in claim 35, wherein the plurality of instructions further include instructions that, when executed by the one or more processors, causes the one or more processors to perform acts including allowing the first computing device to remove a filter from the set of filters imposed by the first computing device but not allowing the second computing device to remove the filter.

**37.** One or more computer-readable media as recited in claim 35, wherein modifying the set of filters comprises one or more of: adding a new filter to the set of filters, removing a filter from the set of filters, and changing parameters of a filter in the set of filters.

**38.** One or more computer-readable media as recited in claim 35, wherein the plurality of instructions further include instructions that, when executed by the one or more processors, causes the one or more processors to perform acts including preventing the filtered device from modifying the set of filters.

**39.** A method comprising:

maintaining an association of virtual addresses and corresponding network addresses;

making a computing device aware of the virtual addresses;

hiding the network addresses from the computing device;

receiving, from the computing device, a data packet intended for a target computing device corresponding to a target virtual address;

replacing, based on the target virtual address, the target virtual address with the corresponding target network address; and

forwarding the data packet to the target computing device at the target network address.

**40.** A method as recited in claim 39, wherein the replacing comprises performing the replacing transparent to the computing device.

**41.** A method as recited in claim 39, further comprising:

receiving, from a source device, another data packet that is intended for the computing device, wherein the other data packet includes a network address of the source device; and

replacing, based on the network address of the source device, the network address of the source device with a corresponding virtual address.

**42.** A method as recited in claim 39, further comprising:

maintaining, at the computing device, a set of filters that further restrict the ability of the computing device to communicate with other computing devices;

allowing the set of filters to be modified from a remote device; and

preventing the computing device from modifying the set of filters.

**43.** A method as recited in claim 39, further comprising:

maintaining a set of filters that restrict the ability of the computing device to communicate with other computing devices;

allowing multiple remote computing devices, each corresponding to a different managerial level, to modify the set of filters; and

preventing a lower managerial level device from modifying the set of filters in a manner that would result in a violation of a filter added by a higher managerial level device.

**44.** One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 39.

**45.** A network mediator comprising:

a mapping of virtual addresses to network addresses; and

a controller, coupled to the mapping, to,

make a corresponding computing device aware of the virtual addresses,

hide the network addresses from the computing device,

receive, from the computing device, a data packet intended for a target computing device corresponding to a target virtual address,

replace, based on the target virtual address, the target virtual address with the corresponding target network address, and

forward the data packet to the target computing device at the target network address.

**46.** A network mediator as recited in claim 45, wherein the network mediator is communicatively coupled to the computing device.

**47.** A network mediator as recited in claim 45, wherein the computing device includes the network mediator.

**48.** A network mediator as recited in claim 45, further comprising:

a set of filters that further restrict the ability of the computing device to communicate with other computing devices; and

wherein the controller is further to,

allow the set of filters to be modified from a remote device, and

prevent the computing device from modifying the set of filters.